IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Robert Nazzal	Art Unit	: 2134
Serial No.	: 10/701,157	Examiner	: Jason K. Gee
Filed	: November 3, 2003	Conf. No.	: 5548
Title	: FEEDBACK MECHANISM TO MINIMIZE FALSE ASSERTIONS OF A NETWORK INTRUSION		

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF

Pursuant to 37 C.F.R. § 41.41, Applicant responds to the Examiner's Answer dated October 14, 2008 as follows.

(1) Claims 1-9 and 22-25 are patentable over Cooper and Symantec.

Claims 1, 3, 5-9, 22 and 24

1. On page 10, paragraph six and in regards to claims 1-9 and 22-25 in view of Cooper and Symantec, the Examiner asserted that

> **Figure 26 of Cooper depicts a page alerting the user of events and associated anomalies. As can be seen on Figure 26, multiple events are alerted to the user. This alerting page is entitled "Events Summary." On the Table depicted in Figure 26, multiple events are listed. The events are listed under the column in the table entitled "Type." For example, "ACCESS_VIOLATION" and "SECURITY ATTACK" are examples of events.**

Appellant contends that "type" in Fig. 26 of Cooper is not an event as argued by the Examiner. Rather, "type" is a disposition code associated with a disposition which is in turn associated with a rule. For example, Table R refers to a disposition "Probable_Scan" with a code "SECURITY_ATTACK" (Cooper, Table R, p. 35). Similarly Fig. 26 contains an entry Count: 266, Rule: Tcp Blocked Service Response, Disposition: Probable_Scan, Type: SECURITY_ATTACK. The terms "type" and "code" therefore are directed to a categorical grouping of information but do not suggest events.

Cooper's events are more appropriately interpreted as the triggering of the rule resulting in an entry in the table. The summary information in the table of Fig. 26 is a summary of past events and not a "summary of the anomalies identified as part of an event" as required by claim 1. For example, the Tcp Blocked Service response event occurred 6,279 times. Each of these occurrences is a unique event. (Cooper, Fig. 26).

2. On page 11, paragraph six and further in regards to claim 1-9 and 22-25 in view of Cooper and Symantec, the Examiner asserted.

> **As can be seen in Symantec on 4-8 and 4-9, a user can select a "Remember" function on the alert. Symantec on 4-9 recites "If the activity is valid ... and you don't want SAM to alert you of this activity in the future, click Remember... Clicking Remember adds this activity to the Exceptions .... Future attempts ... will not trigger the suspicious activity alert .... see ... Chapter 5 for more information." In Chapter 5, Symantec further goes on to teach on 5-7 that "You can remove exceptions you no longer need or want."**
>
> **As seen in the cited areas of Symantec, a user can snooze future alerts for a "period of time," and this time is based upon when the user removes the specified alert form an exception list.**

By allowing a user to create exceptions to monitoring alerts through one mechanism and later remove them through a different mechanism, Symantec discloses a capability that could be viewed as an on / off toggle, similar to a light switch. Symantec provides two separate mechanisms. The first mechanism allows a user to instruct the system to ignore alerts and the second mechanism allows a user to adjust previous selections made by use of the first mechanism. Under no reasonable interpretation does Symantec disclose a snooze function as required by claim 1. Neither the "Remember function" nor editing of the "exceptions list" meet the claim limitation of "a period of time" because there is no period that can be specified by the either Remember control or the exceptions list that would resume alerting the user. The claim is clearly directed to "a control to permit a user to snooze future alerts related to the event in the summary for a period of time," this is not accomplished by the construction given in Symantec.

Motivation to combine

Appellant stands by the argument raised in the Appeal Brief. Moreover, the examiner also mischaracterized these arguments. The examiner argued in part, that "**The Appellants argue that**

there is no basis for the conclusion that it would be beneficial to snooze alerts because not all alerts are malicious."

However that is not exactly what Appellant argued. Rather, Appellant argued that

> The examiner lays no basis for his conclusion that "**as some anomalies are not necessarily a sign of malicious activity. If this is the case, it would be beneficial to snooze these alerts, as they are not malicious.**" Neither Cooper nor Symantec discloses: "a field that depicts a summary of anomalies identified as part of an event" in the first instance. Nor does either of the references or any combination of their teachings describe: "an alert action region including a control to permit a user to snooze future alerts related to the event in the summary for a period of time." Neither Cooper nor Symantec, as pointed out above, lay any basis for snoozing anomalies.

Therefore, the lack of basis was not that not all alerts are malicious, but that neither reference disclosed, "anomalies as part of an event," "snoozing of future alerts related to the event" and "period of time."

Claims 2 and 23

3. On page 13, paragraph one, and in regards to claims 2 and 23 in view of Cooper and Symantec the Examiner asserted.

> **The Appellants argue that the references do not teach that security policies are based on roles of hosts. However, this is clearly taught in Cooper, as cited in the Office Action. Cooper, in paragraph 100, teaches how policies may be generated in regards to security events and alerts. This paragraph recites "The wizard enables the end user to generate policy based on what can be considered gross characteristics of a network at the IP level, such as, for example ... communities of hosts." As seen in this passage, the policy information regarding security alerts and actions may be based on event and host based policies.**

Claim 2 requires that the "snooze control feature is selected based on event types and roles of hosts." Appellant maintains that neither Symantec or Cooper disclose or suggest a snooze capability as requires by claim 2, see argument above with regard to claim 1.

Further, Symantec teaches presenting an alerts window when "suspicious activity" occurs on a system. (Symantec, 4-9) The exemplary alert states "SAM detected an attempt to modify SAM intercept. The file being affected is 'SAM™ Intercept'. The currently active application is

'Finder'". (Symantec, Fig. 4-9) The alert windows presents allow, deny, and remember option as a response to the suspicious activity.

Cooper discloses "communities of hosts" used for setting up a security policy in the policy generator component. (Cooper, [0100]). However, Cooper does not use security policy directly to evaluate activity, instead Cooper "evaluates policy rules against protocol events to determine if the latter conform to the active security policy." (Cooper, Table A). The policy rules themselves "governs a specific interaction or set of interactions, between two communicating entities." (Cooper, Table A). In other words, Cooper evaluates suspicious activity based on activity between two communicating entities. Therefore, the alerts that are generated are based upon communication between two entities.

The examiner suggests that combining Cooper with Symantec results in the Allow, Deny, Remember functionality applied to the security policy of Cooper and therefore one Allow, Deny, or Remember action would apply across a "community of hosts." Appellant disagrees, instead, Symantec's Allow, Deny, or Remember function applies to the suspicious activity resulting in the alerts. In Cooper, alerts are generated from rules (see, e.g., Cooper, Fig. 28). At most Cooper and Symantec suggest Allow, Deny, or Remember functionality to be applied to communication between two entities (rules) and not to communities of hosts (security policy).

Claims 4 and 25

4. On page 14, paragraph 3, and in regards to claims 4 and 25 in view of Cooper and Symantec the Examiner asserts

> **As seen in Figure 22 of Cooper, the events are listed under the column "Type." The anomalies that classify the event are located to the left of the event, such as the information found in the "Count" and "Disposition" columns. For example, for the first event, "ACCESS_VIOLATION," the anomalies that classify the event are "5 counts of "unauthorized access To UrI."**

As Appellant explained above with regard to claim 1, Cooper's events properly refer to the triggering of the rule resulting in an entry on the table and not the "Type" field which is a categorization of the event based on disposition codes.

(2) Claims 10-14 and 18 are patentable over Cooper and Symantec, and Billhartz.

Appellant contends that for reasons discussed in Appeal Brief that these claims are allowable over the alleged combination of references.

For these reasons, and the reasons stated in the Appeal Brief, Applicant submits that the final rejection should be reversed.

Please apply any charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

December 15, 2008

/Paul Pysher/

Date:_____

Paul A. Pysher
Reg. No. 40,780

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (877) 769-7945